UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,433	02/06/2004	Marcus Leech	57983.000164	5978

7590 12/04/2008

Thomas E. Anderson
Hunton & Williams LLP
1900 K Street, N.W.
Washington, DC 20006-1109

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
12/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/772,433	LEECH, MARCUS	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03 October 2008 has been entered.

Response to Amendment

2. Applicant's amendment filed 03 October 2008 amends claims 1 and 6. Applicant's amendment has been fully considered and entered.

Response to Arguments

3. Applicant's arguments with respect to the 112 rejections are not persuasive because the specification (Page 5, line 15) actually states that "the first and second mask values being equal." In addition, original claim 5 also stated that the first and second masks were equal. Therefore, it is clear that the amendments are wholly unsupported by the specification.

4. Applicant has repeatedly chosen to ignore this recitation as pointed to by the Examiner, and has yet to address this recitation.

5. Applicant argues, "Rogaway does not disclose any function that could be analogized to the presently claimed application of an XOR function to all message blocks of a message." This argument is not persuasive because Rogaway discloses that each message blocks is concatenated (Page 5, checksum generation function). The checksum is then XOR'd with Z[m] (Page 5, calculation of value 'T').

6. Applicant alleges, "Any proposed modification to Rogaway would render the teachings of Rogaway unsatisfactory for its intended purposes." This allegation is completely unsupported by any evidence. Nothing that has been presented by Applicant supports their contention that **any** proposed modification to Rogaway would render the teachings unsatisfactory.

7. Utilizing more than one cryptographic key in Rogaway would hardly render the teachings unsatisfactory for its intended purposes. The security benefits of utilizing multiple keys are well recognized by those of ordinary skill in the art. In addition, utilizing more than one cryptographic key does not change the principle operation, because all aspects of the disclosure remain the same with the exception of using different keys for different cryptographic operations.

8. Applicant argues, "any modification away from that single value key frustrates the intended purpose of having the most efficient possible system with modest memory requirements and limiting processing capability." This is not persuasive because storing an extra cryptographic key would not frustrate the memory requirements of the disclosed system of Rogaway. Typical block cipher keys are 64 bits in length.

9. Applicant argues, "a concatenation operation is very different from an XOR operation in both form and result." In response, Applicant has misinterpreted the application of the reference. The summation of the XOR is meant to read on the claimed concatenation. The Examiner never stated that the XOR operation itself was intended to meet the claimed concatenation, but instead said that it was the XOR-**sum**.

10. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on

combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Rejections - 35 USC § 112

11. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

12. Claims 1, 3-11 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The claims have been amended to require, "whitening the at least one encrypted message block with a second mask value, which is not identical to the first mask value," which is not supported by the specification. To the contrary, the specification (Page 5, line 15) actually states that "the first and second mask values being equal." In addition, original claim 5 also stated that the first and second masks were equal. Therefore, it is clear that the amendments are wholly unsupported by the specification.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

15. Claims 1, 3-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rogaway, in view of Schneier, and further in view of Jutla, U.S. Patent No. 7,093,126. Referring to claims 1, 11, Rogaway discloses encrypting a message by exclusive or'ing a block of the message with a corresponding block of a generated value (Page 5, $M[i] \oplus Z[i]$), which meets the limitation of whitening at least one message block with a first mask value. The result of that exclusive or operation is encrypted (Page 5) using a block cipher (Page 4), which meets the limitation of encrypting the at least one whitened message block using a block cipher and a first key. The result of the encryption is the exclusive or'ed with a corresponding block of the generated value (Page 5), which meets the limitation of whitening the at least one encrypted message block with a second mask value to generate at least one corresponding output ciphertext block. Rogaway discloses that the corresponding block of the generated value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value (Page 5, L), which meets the limitation of the first mask value is computed by applying a XOR function to a first value derived from a nonce value and a second value derived from encrypting a third value using the block cipher and a key, wherein the second mask value is computed by applying a XOR function to a fourth value derived from the nonce value and a fifth value derived from encrypting a sixth value using the

block cipher and a key. Rogaway discloses that each message blocks is concatenated (Page 5, checksum generation function), which meets the limitation of applying a XOR function to all message blocks of a message to compute a XOR-sum. Rogaway does not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to encrypt M[i] $\oplus$ Z[i] (Page 5). However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use multiple keys in the encryption algorithm in order to enhance the strength of the encryption algorithm by making the algorithm more difficult to break. Using only a single encryption key is easier break than using multiple because an attacker would only need to discover the one key as opposed to having to discover every key that is used in the encryption algorithm. Rogaway also does not disclose applying a substitution function to the result of the XOR function on L and R. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a substitution function on the result of the XOR function on L and R because substitution operations are an important part of block cipher algorithms that give them security as taught by Schneier (Page 275). Rogaway does not disclose utilizing different mask values. Jutla discloses a similar block ciphering system wherein in one embodiment identical masks are applied to both the outputs and inputs of the cipher blocks (See Jutla, Figure 10 & Col. 5, lines 29-46), which is similar to the system described by Rogaway (Page 5). In a different embodiment, Jutla discloses applying the preceding cipher block out to the block cipher input and the mask to the cipher block output (See Jutla: Figure 5 & Col. 4, lines 7-23), which meets the limitation of whitening the at least one encrypted message block with a second mask value, which is not identical to the first mask value. It would have been obvious to one of ordinary skill in the art at the time the invention was

made to utilize the alternative embodiment described in Jutla in Rogaway because such a modification would have been obvious and within the skill of one skilled in the art and would have yielded predictable results as taught by Jutla (Col. 5, lines 56-62).

Referring to claim 3, Rogaway discloses that to compute the R value, the nonce is XOR'd with L and the result of the XOR function is encrypted with key K (Page 5), which meets the limitation of the first and fourth values derived from the nonce value are permutations of a binary value computed by encrypting the nonce value using the block cipher and the first key.

Referring to claim 4, Rogaway discloses that the L value is generated by encrypted a finite string (Page 5), but does not disclose that the finite string is randomly generated. It would have been obvious to one of ordinary skill in the art at the time the invention was made to randomly generated the finite string used to calculate the L value in Rogaway such that the finite string would be unpredictable, thus increasing the security of cryptographic algorithm as taught by Schneier (Page 45).

Referring to claim 5, Rogaway discloses encrypting a message by exclusive or'ing a block of the message with a corresponding block of a generated value (Page 5, M[i] $\oplus$ Z[i]). The result of that exclusive or operation is encrypted (Page 5) using a block cipher (Page 4). The result of the encryption is the exclusive or'ed with a corresponding block of the generated value (Page 5), which meets the limitation of the steps of whitening each comprise the step of applying a XOR function.

Referring to claim 6, Rogaway discloses that each message blocks is concatenated (Page 5, checksum generation function). The checksum is then XOR'd with Z[m] (Page 5, calculation of value 'T'), which meets the limitation of applying a third mask value to the XOR-sum. The

result of the XOR function is then encrypted (Page 5, calculation of value 'T'), which meets the limitation of encrypting the masked XOR-sum using the block cipher and the first key. Rogaway does not disclose XOR'ing the result of the encryption with a value. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367).

Referring to claim 7, Rogaway discloses that the corresponding block of the generated value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value (Page 5, L), which meets the limitation of the first/third mask value is computed by applying a XOR function to a first value derived from a nonce value and a second value derived from encrypting a third value using the block cipher and a key, wherein the second/fourth mask value is computed by applying a XOR function to a fourth value derived from the nonce value and a fifth value derived from encrypting a sixth value using the block cipher and a key. Rogaway does not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to encrypt M[i] $\oplus$ Z[i] (Page 5). However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use multiple keys in the encryption algorithm in order to enhance the strength of the encryption algorithm by making the algorithm more difficult to break. Using only a single encryption key is easier break than using multiple because an attacker would only need to discover the one key as opposed to having to discover every key that is used in the encryption algorithm. Rogaway also does not disclose applying a substitution function to the result of the XOR function on L and R. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a

substitution function on the result of the XOR function on L and R because substitution operations are an important part of block cipher algorithms that give them security as taught by Schneier (Page 275).

Referring to claim 8, Rogaway describes the decryption process where cipherblocks are XOR'd with the corresponding block of the generated Z value (Page 5), which meets the limitation of whitening the at least one output ciphertext block with the second mask value. The result of the XOR function is decrypted with the key (Page 5), which meets the limitation of decrypting the at least one whitening ciphertext block using a block cipher and the first key. The decrypted value is then XOR's with the corresponding block of the generated Z value (Page 5), which meets the limitation of whitening the at least one decrypted block with a first mask value to generate at least one corresponding message block.

Referring to claim 9, Rogaway discloses that the block cipher used is the AES block cipher (Page 6, first paragraph), which meets the limitation of the block cipher is AES.

Referring to claim 10, Rogaway discloses that the L and R values are elements of the offset vector Z (page 5), which meets the limitation of the second and fifth values are elements of a vector.

16. Claims 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rogaway, in view of Schneier.

Referring to claims 12, 20, Rogaway discloses that each message blocks is concatenated (Page 5, checksum generation function), which meets the limitation of applying a XOR function to all message blocks of a message to compute a XOR-sum. The checksum is then XOR'd with Z[m] (Page 5, calculation of value 'T'), which meets the limitation of applying a third mask

value to the XOR-sum. The result of the XOR function is then encrypted (Page 5, calculation of value 'T'), which meets the limitation of encrypting the masked XOR-sum using the block cipher and the first key. Rogaway does not disclose XOR'ing the result of the encryption with a value. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367).

Referring to claim 13, Rogaway discloses that the corresponding block of the generated value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value (Page 5, L), which meets the limitation of the first/third mask value is computed by applying a XOR function to a first value derived from a nonce value and a second value derived from encrypting a third value using the block cipher and a key, wherein the second/fourth mask value is computed by applying a XOR function to a fourth value derived from the nonce value and a fifth value derived from encrypting a sixth value using the block cipher and a key. Rogaway does not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to encrypt M[i] $\oplus$ Z[i] (Page 5). However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use multiple keys in the encryption algorithm in order to enhance the strength of the encryption algorithm by making the algorithm more difficult to break. Using only a single encryption key is easier break than using multiple because an attacker would only need to discover the one key as opposed to having to discover every key that is used in the encryption algorithm. Rogaway also does not disclose applying a substitution function to the result of the XOR function on L and R. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a

substitution function on the result of the XOR function on L and R because substitution operations are an important part of block cipher algorithms that give them security as taught by Schneier (Page 275).

Referring to claim 14, Rogaway discloses that to compute the R value, the nonce is XOR'd with L and the result of the XOR function is encrypted with key K (Page 5), which meets the limitation of the first and fourth values derived from the nonce value are permutations of a binary value computed by encrypting the nonce value using the block cipher and the first key.

Referring to claims 15, 16, Rogaway discloses encrypting a message by exclusive or'ing a block of the message with a corresponding block of a generated value (Page 5, M[i] $\oplus$ Z[i]), which meets the limitation of whitening at least one message block with a third mask value. The result of that exclusive or operation is encrypted (Page 5) using a block cipher (Page 4), which meets the limitation of encrypting the at least one whitened message block using a block cipher and a first key. The result of the encryption is the exclusive or'ed with a corresponding block of the generated value (Page 5), which meets the limitation of whitening the at least one encrypted message block with the third mask value to generate at least one corresponding output ciphertext block.

Referring to claim 17, Rogaway discloses that the corresponding block of the generated value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value (Page 5, L), which meets the limitation of the first and second mask values are computed by applying a XOR function to a first value derived from a nonce value and a second value derived from encrypting a third value using the block cipher and a key. Rogaway does not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to

encrypt M[i] $\oplus$ Z[i] (Page 5). However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use multiple keys in the encryption algorithm in order to enhance the strength of the encryption algorithm by making the algorithm more difficult to break. Using only a single encryption key is easier break than using multiple because an attacker would only need to discover the one key as opposed to having to discover every key that is used in the encryption algorithm. Rogaway also does not disclose applying a substitution function to the result of the XOR function on L and R. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a substitution function on the result of the XOR function on L and R because substitution operations are an important part of block cipher algorithms that give them security as taught by Schneier (Page 275).

Referring to claim 18, Rogaway discloses that the block cipher used is the AES block cipher (Page 6, first paragraph), which meets the limitation of the block cipher is AES.

Referring to claim 19, Rogaway discloses that the L and R values are elements of the offset vector Z (page 5), which meets the limitation of the second and fifth values are elements of a vector.

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432